Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

EBIOS®

Abschnitt 1
Einführung

Version 2 – 5. Februar 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01 71 75 84 15 - Fax 01 71 75 84 00

Dieses Dokument wurde vom Beratungsbüro der DCSSI
(SGDN / DCSSI / SDO / BCS)
in Zusammenarbeit mit dem EBIOS-Club erstellt.

Kommentare und Anmerkungen werden gerne unter Einsendung an folgende Adresse entgegengenommen:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
FRANCE

ebios.dcssi@sgdn.pm.gouv.fr

Änderungsprotokoll

Version	Gegenstand der Änderung	Stand
02/1997 (1.1)	Veröffentlichung des Leitfadens "Formalisierung von Bedürfnissen und Identifizierung von Sicherheitszielen" (EBIOS – Expression des besoins et d'identification des objectifs de sécurité).	Genehmigt
23/01/2004	Generalüberarbeitung: - Erläuterungen und Anpassung an die Internationalen Normen über Sicherheit und Risikomanagement - Hervorhebung der Basisverordnungen zur Unterscheidung von allen übrigen zu berücksichtigenden Anforderungen. - Integrierung der Konzepte "Hypothese" und "Sicherheitsvorschriften" (ISO/IEC 15408) - Übernahme der ausgewählten wesentlichen Elemente in die Zielsystemstudie - Verbesserungen bei der Festlegung der Bedarfsskala: Werte, die von der Organisation, bezogen auf ihre unmittelbaren Auswirkungen, als akzeptable Grenzen eingestuft werden. - Integrierung der für jedes Element formalisierten Bedarfe bezogen auf die nachfolgende Aktivität. - Integrierung der Bestimmung des Betriebsmodus' in die Hypothesen. - Anpassung der Konzepte an ISO/IEC 15408: Analysiert wird der Ursprung der Bedrohungen, d. h. die Angriffsmethoden und die bedrohenden Elemente, sowie deren Charakterisierung nach Art (natürlich bedingt, menschlich bedingt, umgebungsbedingt), Ursache (unbeabsichtigt, vorsätzlich bei weiterer Aufsplitterung nach Exposition, verfügbare Ressourcen, Fachkenntnissen und Motivation) und Angriffspotential. - Hervorhebung der nicht berücksichtigten Angriffsmethoden - Formalisierung der Bedrohungen im Sinne von ISO/IEC 15408 (bedrohendes Element, Angriff und Wert bezogen auf die Entitäten), bevor diese dem Sicherheitsbedarf gegenübergestellt werden. - Änderung bezüglich der Gegenüberstellung von Bedrohungen und Bedürfnissen zur Identifizierung von Risiken - Hervorhebung der nicht berücksichtigten Risiken - Integrierung der Festlegung minimaler Sicherheitsziele für die Aktivitäten "Formalisierung von Sicherheitszielen" und "Bestimmung von funktionellen Anforderungen" - Änderung bezüglich der Festlegung von Sicherheitszielen, bei der die Hypothesen, die aus der Sicherheits-Policy erwachsenen Vorschriften, die Zwänge, Basisverordnungen und Risiken berücksichtigt werden - Hinzufügen der Bestimmung von Sicherheitsniveaus, wodurch das Niveau der Sicherheitsziele bestimmt (z. B. unter Berücksichtigung des Angriffspotentials) und ein Gewährleistungsniveau ausgewählt werden kann. - Hinzufügen der Bestimmung funktioneller Sicherheitsanforderungen; dadurch können funktionelle Anforderungen bezogen auf die Sicherheitsziele bestimmt und diese Entsprechung dargestellt werden - Hinzufügen der Bestimmung von Sicherheitsgewährleistungsanforderungen, mit denen eventuelle Gewährleistungsanforderungen festgelegt werden können. Verbesserungen hinsichtlich Form, Anpassungen und geringfügiger Korrekturen (Grammatik, Rechtschreibung, Formulierungen, Gestaltung, Kohärenz usw.)	vom EBIOS-Club genehmigt
05/02/2004	Veröffentlichung der Version 2 des EBIOS-Leitfadens	Genehmigt

Inhaltsverzeichnis

Vorwort

Das ständige Bemühen um eine größere Effizienz bei der Wahrung ihrer Aufgaben hat die verschiedenen staatlichen Stellen veranlasst, zunehmend Mittel der Telekommunikation, Datenverarbeitung und Bürotik einzusetzen. Die umfassende Inanspruchnahme dieser Technologien machen die einzelnen Institutionen von ihren IT-Systemen abhängig und anfällig für die zahlreichen potentiellen Bedrohungen. Diese Tatsache trägt erheblich dazu bei, dass die Risiken, die aus der Verarbeitung, Speicherung und Übertragung von Daten erwachsen, im Kern einer jeden Institution immer mehr zunehmen.

Die neuen Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung [OECD] sind Gegenstand einer Empfehlung internationaler Tragweite. Hauptziel dieser Richtlinien ist die Förderung einer "Sicherheitskultur" als Mittel zum Schutze von IT-Systemen und –netzen. Das bedeutet, dass der Sicherheit zentrale Aufmerksamkeit zu schenken ist und dass neue Denk- und Verhaltensmuster bei der Entwicklung und Nutzung von IT-Systemen und –netzen anzuwenden sind. Zu berücksichtigen sind neun Grundsätze, die sich ergänzen und als Entität betrachtet werden sollten.

Was die Informationsgesellschaft anbelangt, hat der Aktionsplan [eEurope 2005] zum Ziel, öffentliche Online-Dienste und Internetzugänge mit hohen Verbindungsgeschwindigkeiten zu fördern. Dieses Bemühen findet seinen Niederschlag in modernen öffentlichen Online-Diensten ("E-Government", "E-Learning", "E-Health"), einem dynamischen Umfeld für E-Business, einer gesicherten IT-Infrastruktur, einer massiven Bereitstellung von Breitbandzugängen zu fairen Preisen, einem Leistungsvergleich ("Benchmarking") sowie der Verbreitung good practices.

Die französische Regierung stellt sich den Herausforderungen der elektronischen Verwaltung. Es geht darum, die IT-Technik in den Dienst der Modernisierung der öffentlichen Dienstes zu stellen, die Effizienz des staatlichen Handelns auf Verwaltungsebene sowie bei den nachgeordneten Gebietskörperschaften zu steigern und die Qualität der Beziehungen zwischen den einzelnen Organen sowie deren Nutzern zu verbessern. Diese Entmaterialisierung der "öffentlichen Dienste" kann nicht erfolgen, wenn nicht ein Minimum an Aufmerksamkeit der Sicherheit geschenkt wird. Es ist in Frankreich Aufgabe der DCSSI des SGDN, zur interministeriellen Definition und zum Ausdruck der Regierungspolitik auf dem Gebiet der IT-Sicherheit beizutragen.

Das Handeln des Staates kann durch die Risiken, die aus der Nutzung von IT-Systemen erwachsen, in Frage gestellt werden. Aus diesem Grunde ist der Schutz von Informationen und die IT-Sicherheit eine der wichtigsten nationalen Verpflichtungen.

Für Systeme, die als geheim eingestufte Informationen verarbeiten, sieht [IGI 1300] beispielsweise vor, dass IT-Systeme "im Rahmen einer Sicherheits-Policy in Abhängigkeit des jeweils geforderten Sicherheitsgrades zu sichern sind, und zwar insbesondere in Abhängigkeit der Sicherheitsstufe der verarbeiteten Informationen und auf Grundlage einer Risikoanalyse".

Dieses Dokument ist Bestandteil einer Serie methodologischer Leitfäden, die von der DCSSI veröffentlicht wurden. Ziel dieser Leitfäden ist es, zur Verbesserung der IT-Sicherheit öffentlicher oder privater Körperschaften beizutragen. Sie sind jederzeit auf Anfrage bei der DCSSI erhältlich.

Dabei stützen sich die Leitfäden auf Unterlagen, die bereits in großem Umfang innerhalb der Behörden erörtert wurden sowie auf die Erfahrung und das Know-how zahlreicher Industrieunternehmer. Die Autoren sind der Meinung, dass die in den Unterlagen und Methoden vorgestellten Konzepte und Gedanken mit Sorgfalt analysiert wurden, und dass die letztendlich zur Anwendung kommende Struktur der Konsistenz, dem Verständnis und der Nutzerfreundlichkeit zu Gute kommt.

Anmerkung: [In Klammern] zitierte Dokumente erscheinen im Literaturverzeichnis am Ende des Leitfadens. Ein Glossar mit den verwendeten Begriffen und Abkürzungen ist hier ebenfalls zu finden.

1 Einführung

1.1 Maßnahmen zur Risikobewertungs

1.1.1 Die IT-Sicherheit

Bei der IT-Sicherheit geht es in erster Linie und hauptsächlich um Informationen und deren Verarbeitung. Daraus lassen sich unmittelbar die Bedarfe, Anforderungen sowie technischen und organisatorischen Zielsetzungen ableiten. Drei Sicherheitsgrundwerte sind zu berücksichtigen: Die Vertraulichkeit, die Integrität und die Verfügbarkeit sowohl der Informationen als auch der Systeme und Umgebungen, in denen sie verarbeitet werden. In gewissen Fällen kann man sich veranlasst sehen, über noch klar zu definierende Auditmittel nach Bedürfnissen wie Nichtrückweisbarkeit, Bewilligung oder Authentifizierung zu fragen.
Die IT-Sicherheit ist unmittelbar an die Risikobewertung und die Risikobehandlung gebunden. Diese Risiken werden als operationell eingestuft, da sie die Aktivitäten der Behörden und Unternehmen direkt beeinflussen. Institutionen, die Mittel der Informations- und Kommunikationstechnik und insbesondere das Internet zur Durchführung von geschäftlichen Aufgaben und Transaktionen in Anspruch nehmen, sind unmittelbar von der IT-Sicherheit betroffen.

1.1.2 Faktoren und Anwendungsbereiche der IT-Sicherheit

Da die IT-Sicherheit neben der Information auch deren Verarbeitung sowie das System einschließlich Umgebung der umfasst, sind folgende Punkte als sicherheitsrelevante Faktoren hervorzuheben:

- Die Informationen,
- die Methoden, Funktionen oder Anwendungen,
- die Technologie (Hardware und Betriebssysteme),
- die physikalische Umgebung (Gebäude, Büroräume usw.),
- der Faktor Mensch.

Alle genannten Faktoren, von denen einige besonders aktiv sind, wie z. B. die Methoden und der Faktor Mensch, sind eindeutig zu definieren. Jeder Faktor bezieht sich schwerpunktmäßig auf einen speziellen Sicherheitsbereich, spielt aber in allen Bereichen eine mehr oder weniger bedeutende Rolle.
Eine Sicherheits-Policy, die nicht alle genannten Faktoren und Anwendungsbereiche berücksichtigt, wäre labil und unvollständig. Sie würde eine gefährliche Lösung darstellen, da sie ein falsches Gefühl der Sicherheit vermittelt, was einen noch größeren Schaden anzurichten vermag, als gar nichts zu tun.

1.1.3 Genormte Maßnahmen

Seit etwa zehn Jahren werden zahlreiche Bemühungen angestellt, um Vorschriften oder zumindest allgemeine Richtlinien über das IT-Sicherheitsmanagement festzulegen. Diese Bemühungen spiegeln sich in nationalen und internationalen Normen wider (z. B. die Normen [ISO 13335], [ISO 17799]…). Obwohl diese Normen noch nicht vollständig stabil sind und immer wieder überarbeitet werden, ist es empfehlenswert, sie so weit wie möglich zu Rate zu ziehen.

In Frankreich ist die Abfassung eines FEROS Pflicht, sobald ein System als geheim eingestufte Informationen verarbeitet, andernfalls wird sie empfohlen. FEROS ist Bestandteil der für die Zulassung zweckdienlichen Sicherheitsunterlagen im Hinblick auf die Akkreditierung eines Systems.

In den internationalen Normen wird die Sicherheits-Policy eines spezifischen IT-Systems unter die globale Sicherheits-Policy von IT-Systemen im allgemeinen geordnet, die ihrerseits der IT-Sicherheit, der Politik für Informations- und Kommunikationstechnik, der Personalpolitik und der Haushalts- und Finanzpolitik untergeordnet ist. Das gesamte Vorhaben hat nur dann Sinn, wenn die zu definierenden Aktionen in Einklang mit der allgemeinen Firmenpolitik und –strategie stehen; entsprechendes gilt für Behörden.

Die Ausarbeitung der Common Criteria [ISO 15408] hat bewirkt, dass, sowohl bei den Nutzern als auch bei den Herstellern, zunehmend Überlegungen über die IT-Sicherheit angestellt werden. Mit den Common Criteria kann die gebotene Sicherheitsgewährleistung bewertet werden, und zwar sowohl was die Konformität der eingesetzten sicherheitsrelevanten Funktionen anbelangt, als auch um

einzuschätzen, inwieweit diese gegen identifizierte Bedrohungen wirksam sind. Bei ihrer Erstellung durch die DCSSI und die zuständigen amerikanischen, britischen, deutschen, kanadischen und niederländischen Stellen wirkten auch europäische Industrieunternehmer der Informatik mit.

Bestimmte internationale Institutionen drängen auf eine Normung der Verfahren durch die Herausgabe konkreter Grundsätze und Zielsetzungen. Genannt seien die OECD und ihre Grundsätze sowie die Europäische Kommission, die regelmäßig für die Mitgliedsstaaten verbindliche Richtlinien aufstellt. So sind beispielsweise sicherheitsrelevante Maßnahmen bereits beim ersten Gedanken an ein neues IT-System zu ergreifen. Dadurch können beim Entwurf eines IT-Systems die notwendigen sicherheitsrelevanten Elemente zusammen mit den funktionellen und operationellen Elementen bereits zu Beginn der Entwurfsplanung berücksichtigt werden. Maximale Effizienz, minimale Kosten und ein sehr positiver ROI (return on investment) sind die unmittelbaren Folgen. Das Ergreifen sicherheitsrelevanter Maßnahmen sollte überhaupt das gesamte IT-System einschließlich seiner Umgebung und seines opertionellen Kontexts betreffen und alle Niveaus der Organisation und des Systems an sich berühren.

1.2 Die Antwort der DCSSI

Die EBIOS-Methode wurde in diesem Sinne und als Kontinuität der beschriebenen Vorgehensweise entwickelt. Sie kommt im allgemeinen während der Entwurfsphase eines operationellen Entwicklungsplans eines IT-Systems zur Anwendung. Hauptziel dieser Methode ist es, Institutionen aller Art, darunter auch den staatlichen Stellen, die Möglichkeit zu bieten, geeignete Sicherheitsaktionen festzulegen.

EBIOS kann vom Sicherheitsbeauftragten einer Institution angewendet werden und ist in jeder Stufe der Struktur eines zu entwickelnden oder eines bestehenden IT-Systems (Untersysteme, Anwendungen) einsetzbar.

In ihrer ersten Version ermöglichte die EBIOS-Methode vor allem die Festlegung von Sicherheitszielen [FEROS].
Nachdem eine Festlegung von Schutzprofilen (protection profiles) immer notwendiger wurde, und nach Herausgabe der Version 2.0 der Common Criteria [ISO 15408], hat die DCSSI im Jahre 2000 mit der Anpassung der EBIOS-Methode an diese Grundsätze begonnen.

Die Ergebnisse einer EBIOS-Studie liefern die zur Abfassung eines IT-Sicherheit-Lastenheftes des untersuchten Systems (FEROS, Schutzprofil - protection profile - o. ä.) notwendigen Informationen und tragen zudem zur Ausarbeitung einer gesicherten funktionellen Architektur bei. Aus der Sicht einer Evaluierung der Common Criteria liefern die Ergebnisse der Studie die notwendigen Informationen zur Erstellung der Spezifikationen des Evaluationsgegenstandes (Beitrag zur Festlegung der Sicherheitsvorgabe).

Ihrem Sinne und ihrer Gesamtphilosophie gemäß ist die EBIOS-Methode in allen Stufen des IT-Systems – von der globalen IT-Sicherheits-Policy (PSSI) bis hin zur speziellen Anwendung – einsetzbar, ohne dass weder die Formulierung noch die Techniken zu ändern wären. Höchstens einige Anpassungen des Vokabulars könnten notwendig werden, um die Konzepte der Methode genau dem jeweiligen Kontext anpassen zu können. So kann z. B. der Begriff "Funktion", der in der Methode häufig als Gegenstand der Untersuchung erscheint, durch Begriffe wie "Tätigkeitsbereich", "Prozess", "System" o. ä. ersetzt werden.
Um diese Umsetzung zu erleichtern und die Öffentlichkeit über die große Bandbreite der EBIOS-Methodik und –Methoden zu informieren, wurden mehrere Leitfäden "Best practices" zusammengestellt.

1.3 Die Leitfäden der Methode

Die EBIOS[1]-Methode besteht aus fünf sich ergänzenden Abschnitten.

- Abschnitt 1 - Einführung
  In diesem Abschnitt werden der Kontext, die Bedeutung und der Ansatz der EBIOS-Methodik vorgestellt. Vervollständigt wird dieser Abschnitt durch ein Literaturverzeichnis, ein Glossar und ein Abkürzungsverzeichnis.
- Abschnitt 2 - Methodik
  Dieser Abschnitt beschreibt den Ablauf der verschiedenen Aktivitäten der Methode.
- Abschnitt 3 - Techniken
  In diesem Abschnitt werden Mittel zur Umsetzung der Aktivitäten der Methode angeboten. Es ist ratsam, diese Techniken den Anforderungen und Praktiken der jeweiligen Institution anzupassen.
- Abschnitt 4 – Mittel zur IT-Risikobewertung
  Dieser Abschnitt entspricht dem ersten Teil der Wissensdatenbanken der EBIOS-Methode (Entitäten, Angriffsmethoden, Schwachstellen)
- Abschnitt 5 – Mittel für die Behandlung von IT-Risiken
  Dieser Abschnitt entspricht dem zweiten Teil der Wissensdatenbanken der EBIOS-Methode (Sicherheitsziele, Sicherheitsanforderungen, Tabellen zur Festlegung der funktionellen Sicherheitsziele und –anforderungen).

Das vorliegende Dokument entspricht dem ersten Abschnitt der Methode.

[1] EBIOS ist eine Schutzmarke des Generalsekretariats der Nationalen Verteidigung in Frankreich.

2 Vorstellung der EBIOS-Methode

2.1 Was ist die EBIOS-Methode?

EBIOS bedeutet "Expression des Besoins et Identification des Objectifs de Sécurité" (Bedarfsanalyse und Identifizierung der Sicherheitsvorgaben).

Es handelt sich hierbei nicht nur um eine **Methode zur IT-Risikobewertung**, sondern um ein regelrechtes **Hilfstool für den Auftraggeber** (Definition eines Studienumfangs, Bedarfsanalyse, Förderung der Eigenverantwortung der Mitwirkenden, usw.). Dank der Common Criteria und den Fortschritten auf dem Gebiet des IT-Sicherheitsmanagements (z. B. durch die Norm [ISO 17799]) hat sich EBIOS auch zu einer **Methode für die Behandlung von IT-Risiken entwickelt.**

EBIOS ist für den Einsatz durch eine Führungskraft ausgelegt (Projektleiter/-leitung, Zulassungsbehörde des Systems, Führungskraft einer Institution u. ä.). Dank dieser Methode können Sicherheitsziele und –anforderungen gemäß den erkannten bzw. anerkannten Risiken rationalisiert werden.

Im weitesten Sinne kann EBIOS als eine Art Leitfaden verstanden werden, der den Institutionen bei ihrer Sicherheits-Policy die nötige Orientierung bietet. Dank dieser globalen Betrachtungsweise der Sicherungsproblematik können einerseits die bereits vorhandene Sicherheit berücksichtigt und andererseits konsistente Basisverordnungen erstellt werden, auf die zukünftige Maßnahmen aufbauen können.

2.2 Vor Beginn einer EBIOS-Studie

Im Idealfall kann sich die EBIOS-Studie auf verschiedene Unterlagen stützen, die sich auf die Institution an sich, auf ihr IT-System und auf das zu untersuchende System beziehen:

- Die Strategie für das Management,
- die IT-Sicherheits-Policy (PSSI)
- die (zukünftigen bzw. bereits vorhandenen) Allgemeinen Spezifikationen des Systems.

In der Regel sind diese Unterlagen jedoch meist unvollständig. Die Arbeit beginnt also häufig mit dem Zusammensuchen von Elementen, die eigentlich in den genannten Basisunterlagen zusammengefasst sein sollten.

Im Übrigen hängt die Präzision der Studie unmittelbar von der Präzision der Allgemeinen Spezifikationen des Systems ab. So wie ein System, dessen Zweck unbekannt ist, nicht Gegenstand einer funktionellen Studie sein kann, kann es auch nicht Gegenstand einer Sicherheitsstudie sein.

2.3 Welches Ergebnis liefert EBIOS ?

Mit EBIOS soll eine Beweisführung durch Erstellung von durch Behörden überprüfbare Basisverordnungen formalisiert werden.

Mit der EBIOS-Methode können nach Bestimmung der Risikobewertung Sicherheitsziele und -anforderungen identifiziert werden, die die Erstellung folgender Unterlagen ermöglicht:

- Eine IT-Sicherheitsstrategie für das Management.
- Die Sicherheits-Policy oder -Leitlinie.
- Ein IT-Sicherheits-Aktionsplan.
- Ein spezielles Pflichtlastenheft im Hinblick auf die IT-Sicherheit [FEROS], das für Systeme, die als geheim eingestufte Information verarbeiten, Vorschrift ist [IGI 900], und für alle anderen Systeme, z. B bei sensiblen Informationen [REC 901], empfohlen wird.
- Angepasste und berechtigte Spezifikationen für die Projektleitung (Pflichten- bzw. Lastenheft).
- Ein Schutzprofil (Protection Profile) bzw. Sicherheitsvorgaben (Security Target) (im Sinne der Common Criteria [ISO 15408])…

Doch EBIOS bietet noch mehr:

- Einfache, flexible und kohärente Beweisführung,
- Verhandlungs- und Schiedsinstrument beim IT-Sicherheits-Prozess,
- Mittel zur Vereinheitlichung des Vokabulars, der Konzepte und der Interpretation des Systems,
- Vorgehen zur Sensibilisierung, Einbindung und Förderung der Eigenverantwortung aller Mirtwirkenden,
- Mit bereits vorhandenen IT-Sicherheits-Tools ([PSSI], [TDBSSI], [MASSIA], [MAQSSIA], [ISO 15408], [ISO 17799]…) kompatibles Tool.

2.4 Was die EBIOS-Methode nicht ermöglicht

Die EBIOS-Methode ist jedoch kein Katalog mit gebrauchsfertigen Lösungen oder Vorschriften in Sachen IT-Sicherheit. Es handelt sich keinesfalls um eine "Wundertüte" mit Ein- und Ausgabe. Sicherheitsprobleme lassen sich nicht durch sofortige Allgemeinlösungen lösen. Mit EBIOS werden zunächst die Sicherheitsanforderungen ermittelt, um anschließend entsprechende Maßnahmen spezifizieren zu können, die aber erst nach Abschluss der Studie zur Anwendung kommen.

2.5 Was die EBIOS-Methode ermöglicht

2.5.1 Unterstützung des Auftraggebers

- Die EBIOS-Methode hilft bei der Definition von Aufgaben, die der Auftraggeber wahrzunehmen hat:
- Festlegung des Untersuchungsgegenstandes unter Beachtung des gesamten Systemkontextes,
- Formalisierung von Bedürfnissen (zu schützender Güter),
- Identifizierung der Bedrohungen,
- Festlegung angemessener Sicherheitsaktivitäten,
- Festlegung der zur Abfassung eines [FEROS] oder Schutzprofils (protection profile) nützlichen Spezifikationselemente,
- Definition eines Projekt- und Verantwortungsplans.

2.5.2 Bereitstellung eines Bewertungs- und Selektionstools für die Projektleitung

- Mit EBIOS kann die Projektleitung:
- die vom Auftraggeber definierten Ziele verfolgen,
- Antworten auf die Durchführbarkeit sowie die damit verbundenen Kosten und Fristen finden,
- Lösungen auswählen,
- Sicherheitsvorgaben (Security Target) bestimmen.

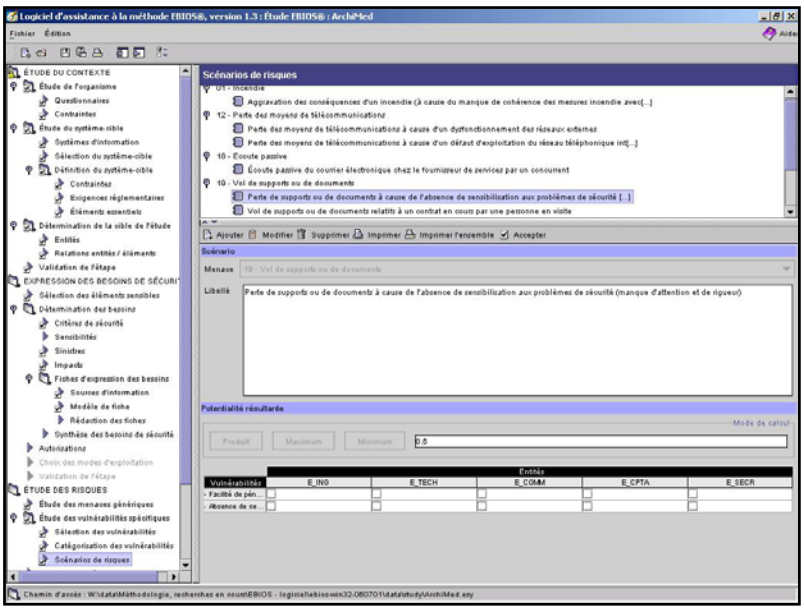
2.5.3 Bereitstellung eines Tools zur Evaluierung der Auswirkungen und zur Verhandlung zwischen Auftraggeber und Führungskräften (des Projekts, der Institution…)

EBIOS hilft den Führungskräften:

- die Auswirkungen auf die Umgebung zu beurteilen,
- die Angemessenheit der IT-Systeme zu kontrollieren,
- die Untersuchungen und die IT-Sicherheit zu zentralisieren,
- strategische sicherheits- und verfahrensrelevante Entscheidungen zu treffen.

3 Tools der EBIOS-Methode

3.1 Freie Software



Die EBIOS-Software erleichtert die Durchführung einer EBIOS-Studie ungemein. Mit dem Programm können Studienergebnisse festgehalten und entsprechende Synthesedokumente erstellt werden. Dank intuitiver Handhabung lassen sich die Wissensdatenbanken individuell gestalten.

Es handelt sich um eine freie, kostenlose erhältliche Software einschließlich Quellcodes, das auf einfache Anfrage unter Angabe der persönlichen Daten über ebios.dcssi@sgdn.pm.gouv.fr. bezogen werden kann.

In Java und XML geschrieben, kann das Programm von den Nutzern jederzeit verbessert werden, indem Rückmeldungen an das SGDN übermittelt werden.

3.2 Best practices

Die EBIOS-Methode stellt gewissermaßen einen modularen Werkzeugkasten dar. Je nach Liefergegenstand können der Ablauf und die Feinheiten der Methode variieren. Diesbezüglich wurden mehrere Leitfäden ("Best practices") zusammengestellt, in denen erklärt wird, wie die Ergebnisse der EBIOS-Methode je nach gewünschtem Zweck bestmöglichst genutzt werden können.

- Festlegung einer IT-Sicherheitsstrategie für das Management
- Festlegung einer IT-Sicherheits-Policy (PSSI)
- Abfassung eines FEROS
- Abfassung eines SSRS (*System-specific Requirement Statement* – NATO)
- Abfassung eines Schutzprofils (Protection Profiles) (nach ISO/IEC 15408)
- Abfassung von Sicherheitsvorgaben (Security Targets) (nach ISO/IEC 15408)
- Schaffung eines Rahmens zum Informations-Sicherheitsmanagement
- Abfassung einer Zertifizierungspolitik
- Untersuchung eines zu entwickelnden Systems
- Untersuchung eines bereits bestehenden Systems...

Alle Unterlagen sind über das Internet erhältlich (http://www.ssi.gouv.fr/).

3.3 Schulung

Das Schulungszentrum der DCSSI (CFSSI genannt) bietet Kurse an, in denen Vertreter des französischen öffentlichen Dienstes die EBIOS-Methode erlernen können.

Zur Weitergabe von Kenntnissen und zur Vermeidung von eventuellen Abweichungen bei der Verbreitung und dem Gebrauch der Methode bietet die DCSSI auch Schulungen für Ausbilder an.

Informationen über die Schulungen sind im Internet über die Adresse http://www.ssi.gouv.fr/formation erhältlich.

3.4 EBIOS-Club

2003 wurde der Club der Anwender der EBIOS-Methode gegründet. Die Experten der Methode haben bei diesen Treffen die Möglichkeit, Erfahrungen auszutauschen und die Methode bzw. ihre Arbeitsmittel weiter zu entwickeln.

Glossar

Die französiche Originalbezeichnung sowie die englische Übersetzung der im Glossar aufgeführten Begriffe stehen in Klammern. Beispiele sind kursiv gedruckt. Der in den Definitionen unterstrichene Text entspricht den im vorliegenden Text definierten Konzepten.

Angriffsmethoden
(méthode d'attaque; attack method)

Typisches Mittel (Aktion oder Ereignis) eines bedrohenden Elements, einen Angriff durchzuführen.

Beispiele:

- *Diebstahl von Unterlagen oder Dokumenten,*
- *Einrichten von Software-Schwachstellen*
- *Beeinträchtigung der Personalverfügbarkeit,*
- *passives Mithören,*
- *Hochwasser,*
- *…*

Angriff
(attaque; attack)

Ausnutzung einer oder mehrerer Schwachstellen mittels einer Angriffsmethode bei sich bietender Wahrscheinlichkeit.

Beispiele:

- *Die Wahrscheinlichkeit, gefälschte oder kopierte Software zu benutzen, ist günstig, da keine Sensibilisierungs- bzw. Aufklärungsarbeit hinsichtlich der Gesetzgebung über Urheberrechte geleistet wurde.*
- *Programmschädigung durch Viren auf Grund der Einfachheit, mit der Schad-Software in das IT-Netz der Institution eingeschleust werden kann.*
- *…*

Auswirkung
(impact; impact)

Auswirkung auf die Institution bei Konkretisierung einer Bedrohung.

Beispiele:

- *Imageverlust bei den Kunden,*
- *Finanzielle Verluste in Höhe von 10 % des Umsatzes,*
- *Verstoß gegen Gesetze und Vorschriften mit gerichtlicher Verfolgung des Direktors als unmittelbare Folge,*
- *…*

Bedrohendes Element
(élément menaçant; threat agent)

Menschliches Handeln oder natürliches bzw. umgebungsbedingtes Phänomen mit potentiell negativen Auswirkungen auf das System. Durch ihre Art (natürlich bedingt, menschlich bedingt oder umgebungsbedingt) und ihre Ursache (unbeabsichtigt oder vorsätzlich charakterisierbar. Bei unbeabsichtigter Ursache sind die Faktoren Exposition und verfügbare Ressourcen zu berücksichtigen. Bei vorsätzlicher Ursache sind die Faktoren Fachkenntnisse, verfügbare Ressourcen und Motivation zu berücksichtigen.

Beispiele:

- *Ehemaliger Mitarbeiter mit geringem technischen Sachverstand und wenig freier Zeit, aber möglicherweise hoher Motivation;*
- *Hacker mit hohem technischen Sachverstand, guter Ausstattung und hoher Motivation in Anbetracht des zu verdienenden Geldes;*
- *sehr feuchtes Klima während 3 Monaten im Jahr;*
- *Viren;*
- *Nutzer;*
- *Software-Entwickler;*
- *…*

Bedrohung
(menace; threat)

Möglicher Angriff eines bedrohenden Elements auf ein Wert.

Beispiele:

- *Ein ehemaliger Mitarbeiter mit geringem technischen Sachverstand aber vermutlich hoher Motivation beeinträchtigt vorsätzlich die Systemsoftware mit einem Virus, indem er sich die Einfachheit zu Nutze macht, mit der Schad-Software in das IT-Netz der Institution eingeschleust werden kann; davon betroffen werden könnten Funktionen wie z. B. die Erstellung von Kostenvoranschlägen oder die Erzeugung von Signaturzertifikaten.*
- *Ein Hacker mit guten Fachkenntnissen und Standardausstattung, der dafür bezahlt wird, eignet sich unrechtmäßig vertrauliche Dateien an, indem er das Firmennetz per Fernzugriff anzapft.*
- *Ein Software-Entwickler, Mitarbeiter der Firma, mit sehr guten Kenntnissen der Quellcodes aber nur geringen IT-Sicherheits-Kenntnissen ändert vorsätzlich den Quellcode.*
- *Ein Besucher entwendet Unterlagen, die vertrauliche Informationen enthalten.*
- *…*

Nutzer
(utilisateur; user)

Personen oder Objekte, die die Dienste einer Organisation in Anspruch nehmen.

Eingehen eines Risikos
(prise de risque; risk retention)

Akzeptanz der aufgrund eines bestehenden Risikos evtl. entstehenden Verluste

Entität
(entité; entity)

Es handelt sich um ein Wert das als Organisation, Standort, Personal, Hardware, Netz, Software, System auftreten kann.

Beispiele:

- *IT-Dienstleister,*
- *Büroräume der Organisation,*
- *System-Administrator,*
- *Laptop,*
- *Ethernet,*
- *Betriebssystem,*
- *Portal für Teleprozeduren*
- *…*

Exposition
(exposition; exposure)

Natürliches Expositionsniveau eines Zielsystems gegenüber einem bedrohenden Element bei unbeabsichtigter Ursache. Dabei kann das Niveau mit geringer, mittlerer oder großer Exposition umschrieben werden.

Beispiele:

- *geringe Exposition,*
- *mittlere Exposition,*
- *große Exposition.*

Fachkenntnisse
(expertise; expertise)

Technischer Sachverstand eines bedrohenden Elements bei vorsätzlicher Ursache. Dabei kann der erwartete Grad technischen Sachverstands als gering, mittel oder hoch Sachverstand eingestuft werden.

Beispiele [Guide 650]:

- *geringer technische Sachverstand,*
- *mittlerer technische Sachverstand,*
- *hoher technische Sachverstand.*

Funktion
(fonction; function)

Handlung, bei der Informationen angelegt, geändert, gelöscht oder transportiert werden, die zum reibungslosen Ablauf einer Aktivität einer Institution beiträgt.

Beispiele:

- *Anlegen technischer Pläne,*
- *Erstellen von Kostenvoranschlägen,*
- *Rechnungsführung,*
- *Verschlüsselungsalgorithmus,*
- *Ausstellen eines Zertifikats,*
- *…*

Funktionelle Sicherheitsanforderung
(exigence fonctionelle de securité; security functional requirement)

Funktionelle Spezifikation der zu ergreifenden Sicherheitsfunktionen zur Verfolgung eines oder mehrerer Sicherheitsziele in bezug auf das Zielsystem.

Beispiele:

- *Das System muss die Chiffrierschlüssel entsprechend eines spezifizierten Algorithmus zur Schlüsselerzeugung sowie spezifizierten Schlüssellängen in Einklang mit den spezifizierten Normen erzeugen.*
- *Das System muss ein physikalisches, evtl. systemstörendes Eindringen eindeutig detektieren können.*
- *Die Räumlichkeiten der Institution müssen mit Blitzableitern ausgerüstet sein.*
- *…*

Wahrscheinlichkeit
(opportunité; opportunity)

Wahrscheinlichkeit, mit der ein Angriff zu erwarten ist.

Beispiele:

- *Unwahrscheinlich,*
- *sehr wahrscheinlich,*
- *völlig unmöglich,*
- *zu 15 % wahrscheinlich,*
- *…*

Wert
(bien; asset)

Mittel aller Art, die für die Organisation einen Wert darstellen und die zum Erreichen der festgelegten Ziele notwendig sind. Es ist zwischen zu schützenden wesentlichen Elementen und Entitäten zu unterscheiden.

Beispiele:

- *Namenslisten,*
- *Zertifizierungsgesuche,*
- *Rechnungsführung,*
- *Verschlüsselungsalgorithmus,*
- *Laptop,*
- *Ethernet,*
- *Betriebssystem,*
- *…*

Hypothese
(hypothèse; assumption)

Postulat bezüglich der operationellen Umgebung des Systems zur Bereitstellung der erwarteten Sicherheitfunktionalitäten.

Beispiele:

- *Das System wird in einem Raum untergebracht, der speziell zur Minimierung elektromagnetischer Abstrahlungen entwickelt wurde.*
- *Der Administrator wird in einem Bereich mit begrenztem Zugang untergebracht;*
- *Die Nutzer schreiben ihr Passwort nicht auf.*

- *Das Hausnetz wird an kein anderes Netz angeschlossen, das nicht als sicher geprüft wurde.*
- *Jeder Mitarbeiter kennt seine Aufgaben im Falle der unerlaubten Verbreitung von Betriebsgeheimnissen oder der illegalen Manipulation betriebswichtiger Daten.*
- *…*

Identifizieren der Angriffsquellen
(identification des origines des attaques; source identification)

Verfahren zum Auffinden, Erfassen und Charakterisieren von Angriffsquellen (Bedrohende Elemente und Angriffsmethoden)

Information
(information; information)

Auskunft oder Wissenselement, das in einer der Kommunikation, Aufzeichnung oder Verarbeitung angepassten Form dargestellt werden kann. [IGI 900] [REC 901]

Beispiele:

- *Eine Meldung,*
- *eine Namensliste,*
- *ein Zertifizierungsgesuch,*
- *eine Widerrufsliste,*
- *…*

IT-System
(système d'information; information system)

Gesamtheit aller Entitäten, die zur Sicherstellung von Funktionen der Informationsverarbeitung eingesetzt werden.

Integrität
(intégrité; integrity)

Eigenschaft der Genauigkeit und Vollständigkeit der wesentlichen Elemente.

Motivation
(motivation; motivation)

Motiv eines bedrohenden Elements. Es kann strategischer, ideologischer, terroristischer, habgieriger, spielerischer oder sich rächender Natur sein und ist verschieden, je nachdem, ob es sich um eine unbeabsichtigte (Neugierde, Langeweile...) oder vorsätzliche (Spionage, Verlockung des Geldes, Schädigungsabsicht, Ideologie, Spielerei, Betrügerei, Diebstahl, Piraterie, intellektuelle Herausforderung, Rache, Vorrat; Erpressung von Geld...) Tat handelt.

Beispiele [Guide 650]:

- *Strategischer Natur,*
- *ideologischer Natur,*
- *terroristischer Natur,*
- *habgieriger Natur,*
- *spielerischer Natur,*
- *sich rächender Natur.*

[…]

- *Vorsätzliche Taten:*
  - *Spionage,*
  - *Verlockung des Geldes,*
  - *Schädigungsabsicht,*
  - *Ideologie,*
  - *Spielerei,*
  - *Betrügerei,*
  - *Diebstahl,*
  - *Piraterie,*
  - *intellektuelle Herausforderung,*
  - *Rache,*
  - *Verrat,*
  - *Erpressung von Geld.*
  - *…*

- *Unbeabsichtigtee Taten:*
  - *Neugierde,*
  - *Langeweile,*
  - *…*

Restrisiko
(risque résiduel; residual risk)

Noch verbleibendes Risiko nach erfolgter Risikobehandlung. [ISO Guide 73]

Risiko
(risque; risk)

Zusammenspiel einer Bedrohung und der daraus evtl. entstehenden Verluste, d. h. einer Wahrscheinlichkeit zur Ausnutzung einer oder mehrerer Schwachstellen einer oder mehrerer Entitäten durch ein bedrohendes Element unter Einsatz einer Angriffsmethode und ihrer Auswirkung auf die wesentlichen Elemente sowie die Institution an sich.

Beispiele:

- *Ein ehemaliger Mitarbeiter mit geringem technischen Sachverstand aber vermutlich hoher Motivation beeinträchtigt vorsätzlich die Systemsoftware mit einem Virus, indem er sich die Einfachheit zu Nutze macht, mit der Schadsoftware in das IT-Netz der Institution eingeschleust werden kann; davon betroffen werden könnten z. B. die Verfügbarkeit und Integrität der Funktion zur Erstellung von Kostenvoranschlägen oder zur Erzeugung von Signaturzertifikaten, was zur Folge hätte, dass ein Dienst nicht erbracht oder einer vertraglichen Verpflichung nicht nachgekommen werden könnte, was wiederum bedeutende Imageverluste mit sich bringen würde.*
- *Ein Hacker mit guten Fachkenntnissen und Standardausrüstung, der dafür bezahlt wird, eignet sich unrechtmäßig vertrauliche Dateien an, indem er das Firmennetz per Fernzugriff anzapft; das dadurch verursachte Misslingen einer Transaktion mit einem Geschäftspartner hat wiederum einen Imageverlust zur Folge.*
- *…*

Risikoakzeptanz
(acceptation de risque; risk acceptance)

Beschluss, ein gemäß den Risikokriterien behandeltes Risiko zu tolerieren

Risikoanalyse
(analyse de risque; risk analysis)

Systematische Datenauswertung zur Identifizierung der Angriffsquellen und zur Risikoeinschätzung.

Risikobehandlung
(traitement de risque; risk treatment)

Prozess der Auswahl und Durchführung von Maßnahmen zur Änderung des Risikos, z. B. Risikominderung, Risikotransfer oder Eingehen eines Risikos.

Risikoeinschätzung
(estimation de risque; risk estimation)

Prozess, um die Eintrittswahrscheinlichkeit und die Verluste, die ein Risiko mit sich bringen kann, bewerten zu können.

Risikoevaluierung
(évaluation du risque; risk evaluation)

Prozess, bei dem das eingeschätzte Risiko mit den gegebenen Risikokriterien verglichen wird, um die Bedeutung eines Risikos festzulegen. [ISO Guide 73]

Risiko-Kommunikation
(communication relative au risque; risk communication)

Austausch bzw. Weitergabe von risikospezifischen Informationen zwischen Entscheidungsträger und übrigen Beteiligten. [ISO Guide 73]

Risikokriterien (critères de risque; risk criteria)	Referenzbegriffe zur Bestimmung des Ausmaßes der Risiken.
Risikomanagement (gestion du risque; risk management)	Koordinierte Aktivitäten zur Steuerung und Lenkung einer Institution hinsichtlich eines Risikos. Das Risikomanagement umfasst generell die Risikobewertung, die Risikobehandlung, die Risikoakzeptanz und die Risiko-Kommunikation. [ISO Guide 73]
Risikominderung (réduction du risque; risk reduction)	Prozess, der die negativen Konsequenzen und die Wahrscheinlichkeiten einer Bedrohung minimieren soll.
Risikotransfer (transfert du risque; risk transfer)	Verteilung der durch ein eingegangenes Risiko evtl. entstehenden Verluste gegenüber einem Dritten. *Beispiele:* - *Abschließen einer Versicherung,* - *…*
Schwachstellen (vulnérabilité; vulnerability)	Eigenschaft einer Entität, die hinsichtlich der IT-Sicherheit eine Schwäche bzw. Lücke darstellen kann. *Beispiele:* - *Fehlende Brandschutzorganisation bei einer Entität des Typs "Organisation".* - *Geringe Sensibilisierung für sicherheitsgerechtes Verhalten bei einer Entität des Typs "Personal".* - *Leichtigkeit, mit der in eine Entität des Typs "Standort" eingedrungen werden kann.* - *Möglichkeit, Systembefehle für eine Entität des Typs "Netz" zu erzeugen bzw. zu ändern.* - *…*
Sicherheitsanforderung (exigence de sécurité; security requirement)	Funktionelle Spezifikation bzw. Gewährleistungsspezifikation über das IT-System bzw. dessen Umgebung, die die zu ergreifenden Sicherheitsmechanismen beschreibt und ein oder mehrere Sicherheitsziele verfolgt.
Sicherheitsbedarf (besoin de sécurité; sensitivity)	Klare und eindeutige Definition der den Sicherheitsgrundwerten (Verfügbarkeit, Vertraulichkeit, Integrität, ...) entsprechenden Niveaus, die für ein wesentliches Element zu gewährleisten sind.
Sicherheitsgewährleistungsanforderung (exigence d'assurance de sécurité; security assurance requirement)	
Sicherheitsgrundsatz (principe de sécurité; security principle)	Die Sicherheitsgrundsätze sind Ausdruck der notwendigen Sicherheitsorientierungen und der wesentlichen Sicherheitsmerkmale zur Ausarbeitung einer Sicherheits-Policy und insbesondere der sie konstituierenden Sicherheitsvorschriften. [PSSI]

Sicherheitsgrundwert	Eigenschaft eines wesentlichen Elementes zur Beurteilung der verschiedenen Sicherheitsbedarfe .
Sicherheitsmaßnahme (mesure de sécurité; security measure)	Mittel zur Verbesserung der Sicherheit, das durch eine Sicherheitsanforderung spezifiziert und zur Umsetzung dieser Anforderung eingesetzt wird. Dabei kann es sich um vorbeugende, vorbereitende, abschreckende, schützende, auffindende, eingrenzende, "bekämpfende", wiederverwendende, wiederaufbereitende, kompensierende, ... Maßnahmen handeln.
IT-Sicherheits-Policy (politique de sécurité de système d'information ; information systems security policy)	Gesamtheit aller strategischen Elemente, Richtlinien, Verfahren, Verhaltenskodexe, organisatorischen und technischen Vorschriften, die – in einem anzuwendenden Dokument definiert – zum Ziel haben, das / die IT-System(e) der Institution zu schützen. [PSSI]
Risikobewertung (appréciation de risque; risk assessment)	Zusammenspiel von Risikoanalyse und Risikoeinschätzung. [ISO Guide 73]
Sicherheitsvorschrift (règle de sécurité; organisational security policy)	Sicherheits-Vorschrift, -Verfahren, -Verhaltenskodex oder -Richtlinie, die eine Organisation für ihren ordnungsgemäßen Betrieb vorschreibt. [ISO 15408] *Beispiele:* - *Alle vom Staat zur Erzeugung von Passwörtern und bei der Kryptologie eingesetzten Mittel müssen den nationalen Normen entsprechen.* - *Alle im Bankwesen eingesetzten Mittel müssen EAL4-zertifiziert sein, erhöht um die Versicherungselemente ADV_IMP.2.* - *Die Zugangskontrolle erfolgt über Nutzeridentifikation / Passwort.* - *Jeder Ingenieur ist für die von ihm bearbeitete Datei verantwortlich.* - *Außerhalb der Öffnungszeiten (19h – 7h) muss eine Einbruchmeldeanlage aktiviert sein.* - *…*

Sicherheitsziel
(objectif de sécurité; security objective)

Ausdruck der Absicht, (je nach Kontext) erkannte Bedrohungen oder Risiken auszuschalten und/oder der organisatorischen Sicherheits-Policy bzw. den Hypothesen gerecht zu werden; das Sicherheitsziel kann sich auf das Zielsystem an sich, dessen Entwicklungsumgebung oder operationelle Umgebung beziehen.

Beispiele:

- *"Offene" Ziele (großer Handlungsspielraum bei Verfolgung des Sicherheitsvorgabe):*
  - *Die Arbeitsplatzkonfigurationen innerhalb des internen Netzes müssen weiterentwicklungsfähig sein.*
  - *Die Räume sind gegen Blitzeinschlag zu schützen.*
  - *…*
- *"Geschlossene" Ziele (geringer Handlungsspielraum bei Verfolgung der Sicherheitsvorgabe):*
  - *Das System muss die Nutzer eindeutig identifizieren und authentifizieren können, und zwar vor Beginn einer Interaktion zwischen System und Nutzer.*
  - *Zwei verschiedene, kompatible Antivirenprogramme sind zu installieren, die Virussignaturen sind alle zwei Wochen zu aktualisieren.*
  - *…*

IT-Sicherheit
(sécurité des systèmes d'informations (SSI); information security)

Schutz von IT-Systemen, und insbesondere der wesentlichen Elemente, gegen unzulässige (vorsätzliche oder unbeabsichtigtee) Beeinträchtigungen der Sicherheitsgrundwerte.

Verfügbare Ressourcen
(ressources disponibles ; available resources)

Erwartete Mittel eines bedrohenden Elements. Das Niveau der verfügbaren Ressourcen entspricht dem Angriffspotential und kann nach geringen, mittleren und großen Ressourcen unterschieden werden.

Beispiele:

- *Geringe Ressourcen,*
- *mittlere Ressourcen*
- *große Ressourcen.*

Verfügbarkeit
(disponibilité; availability)

Eigenschaft der Zugänglichkeit der wesentlichen Elemente durch autorisierte Nutzer zu einem bestimmten Zeitpunkt.

Vertraulichkeit
(confidentialité; confidentiality)

Eigenschaft der wesentlichen Elemente, nur den autorisierten Nutzern zugänglich zu sein.

Wesentliches Element
(élément essentiel; essential element)

Daten oder eine Funktion, dessen Sicherheitsbedarf zumindest nicht gleich Null ist.

Beispiele:

- *eine Namensliste,*
- *ein Zertifizierungsgesuch,*
- *die Rechnungsführung,*
- *ein Verschlüsselungsalgorithmus,*
- *…*

Abkürzungen

BCS	Beratungsbüro zur IT-Sicherheit (Bureau Conseil en Sécurité des systèmes d'information)
CC	*Common Criteria*; gebräuchliche Bezeichnung für die offizielle ISO-Bezeichnung: "Prüfkriterien zur Beurteilung der Sicherheit von Informationstechnologien".
CFSSI	Ausbildungszentrum zur IT-Sicherheit (Centre de Formation en Sécurité des Systèmes d'Information)
DCSSI	Zentrale Direktion für die IT-Sicherheit (Direction Centrale de la Sécurité des Systèmes d'Information)
EBIOS	Formalisierung von Bedürfnissen und Identifizierung von Sicherheitszielen (Expression des Besoins et Identification des Objectifs de Sécurité)
FEROS	Spezielles Pflichtlastenheft im Hinblick auf die IT-Sicherheit (Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI)
IKT	Informations- und Kommunikationstechnik (Technologies de l'Information et de Communication)
PP	*Protection Profile* – Schutzprofil
PSSI	IT-Sicherheits-Policy (Politique de Sécurité des Systèmes d'Information)
SDO	Verfahrensausschuss (Sous-Direction des Opérations)
SDSSI	Leitschema zur IT-Sicherheit (Schéma Directeur de la Sécurité des Systèmes d'Information)
SGDN	Generalsekretariat der Nationalen Verteidigung in Frankreich (Secrétariat Général de la Défense Nationale)
SSI	IT-Sicherheit (Sécurité des systèmes d'information)

Literaturverzeichnis

[eEurope 2005] *Plan d'action eEurope 2005 : une société de l'information pour tous, COM(2002)263 final* – Commission européenne (2002).

[FEROS] *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS)* – SGDN/SCSSI (1991).

Im Internet über http://www.ssi.gouv.fr erhältlich.

[Guide 650] *La menace et les attaques informatiques* – N°650 / DISSI / SCSSI (1994).

Im Internet über http://www.ssi.gouv.fr erhältlich.

[IGI 1300] *Instruction générale interministérielle sur la protection du secret de la défense nationale* – N°1300 / SGDN / PSE / SSD (2003).

[IGI 900] *La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées* – SGDN et DISSI (1993).

[ISO 13335] *Information technology – Security techniques – Guidelines for the management of IT security (GMITS)* – International Organization for Standardization (ISO) (2001).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information*, – International Organization for Standardization (ISO) – version 2.0 (1998).

[ISO 17799] *Information technology – Code of practice for information security management* – International Organization for Standardization (ISO) (2000).

[ISO Guide 73] *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes* – International Organization for Standardization (ISO) (2002).

[MASSIA] *Méthode d'Audit de la Sécurité des Systèmes d'Information de l'Armement* – CELAR/CASSI/GESSI – version 1.0 (1994).

[OCDE] *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* – Organisation de coopération et de développement économiques (OCDE) (2002).

[PSSI] *Guide d'élaboration de politique de sécurité de système d'information* – DCSSI (2004).

Im Internet über http://www.ssi.gouv.fr erhältlich.

[REC 901] *Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense* – SGDN et DISSI (1994).

TDBSSI *Guide d'élaboration de tableaux de bord de sécurité de système d'information pour les administrations* – DCSSI (2004).

Im Internet über http://www.ssi.gouv.fr erhältlich.

Formular zur Meinungsäußerung

Dieses Formular kann an folgende Adresse gesendet werden:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identifizierung der Beitrags
Name und Institution (fakultativ): .....
Elektronische Adresse: .....
Datum: .....

Allgemeine Bemerkungen zu diesem Dokument
Entspricht das Dokument Ihren Bedarfe? Ja ☐ Nein ☐

Wenn ja:

Glauben Sie, dass es vom Inhalt her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

Was haben Sie vermisst?
.....
.....

Welche Teile des Dokuments erscheinen Ihnen überflüssig oder unangemessen?
.....
.....

Glauben Sie, dass es von der Form her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

In welchem Bereich ist es verbesserungsfähig?
- Leserlichkeit, Verständnis ☐
- Aufmachung ☐
- Sonstiges ☐

Formulieren Sie Ihre Wünsche bezüglich der Form:
.....
.....

Wenn nein:

Geben Sie den Bereich an, der Ihnen nicht gefällt und umschreiben Sie, was Ihnen gefallen hätte:
.....
.....

Welche weiteren Themen hätten Sie gerne vorgefunden?
.....
.....

Spezielle Bemerkungen zu diesem Dokument

In nachstehender Tabelle können Sie detailliert Stellung nehmen.

Unter Nr. ist die Laufnummer einzutragen.

In die Spalte "Typ" sind zwei Buchstaben einzutragen:

Mit dem ersten Buchstaben wird die Kategorie der Bemerkung umschrieben:

- R Rechtschreib- oder Grammatikfehler
- E Mangelnde Erläuterung oder Klärung des behandelten Punktes
- U Text unvollständig oder nicht vorhanden
- F Fehler

Der zweite Buchstabe beschreibt den Bedeutungsgrad:

- g geringfügig
- G Gravierend

Unter "Referenz" ist die genaue Lokalisierung im Text anzugeben (Kapitelnummer, Zeile...).

Unter "Wortlaut der Bemerkung" kann ein Kommentar abgegeben werden.

Unter "vorgeschlagene Lösung" können Mittel zur Lösung des aufgeworfenen Problems angegeben werden.

Nr.	Typ	Referenz	Wortlaut der Bemerkung	Vorgeschlagene Lösung
1				
2				
3				
4				
5				

Vielen Dank für Ihre Teilnahme